
Together we have the opportunity to empower the world
through the use of free software. Read more.

**BECOME A
MEMBER**

172 Joined

600 New Members

Esta es una traducción de la página original en inglés.

El software de Google es *malware*

El software que no es libre (privativo) a menudo es *malware* (diseñado para maltratar a los usuarios). El software que no es libre está controlado por quienes lo han desarrollado, lo que los coloca en una posición de poder sobre los usuarios; esa es la injusticia básica. A menudo los desarrolladores y fabricantes ejercen ese poder en perjuicio de los usuarios a cuyo servicio deberían estar.

Habitualmente, esto suele realizarse mediante funcionalidades maliciosas.

Si conoce algún ejemplo más que deba estar incluido en esta página, escriba por favor a <webmasters@gnu.org> para informarnos. Incluya la URL de una o dos referencias confiables para justificar su inclusión.

[Puertas traseras](#) [Censura](#) [DRM](#) [Fallos de seguridad](#) [Intromisiones](#)
[Sabotaje](#) [Espionaje](#) [Tiranos](#)

Puertas traseras

- Los ChromeBooks están programados para quedar obsoletos: ChromeOS tiene una puerta trasera universal que es utilizada para las actualizaciones y que deja de funcionar en una fecha predeterminada. A partir de ese momento parece que el ordenador deja de recibir toda asistencia.

En otras palabras, cuando uno deja de ser ultrajado por la puerta trasera, empieza a ser ultrajado por la obsolescencia.

- Android tiene una puerta trasera para cambiar de forma remota los ajustes del «usuario».

El artículo sugiere que pudiera tratarse de una puerta trasera universal, pero esto no está claro.

- ChromeOS tiene una puerta trasera universal. Al menos así lo reconoce Google en la sección 4 del Acuerdo de Licencia de Usuario Final.
- En Android, Google ha dispuesto una puerta trasera para borrar aplicaciones de forma remota. (Esto lo hacía con un programa llamado GTalkService, al parecer integrado en Google Play desde entonces).

Google también puede forzar la instalación de programas de manera remota mediante GTalkService. Esto no equivale a una puerta trasera, pero permite

hacer algunos chanchullos.

Aunque de momento Google no haya *ejercido* ese poder de forma tan malintencionada, la cuestión es que nadie debería tener poder para actuar así. Usted bien podría decidir que un servicio de seguridad *desactive* los programas que considere peligrosos. Pero no hay excusa para permitir que *borre* los programas, y usted debe tener derecho a decidir en quién confiar (si es que en alguien) para hacer esto.

Censura

- Google ofrece un software de censura, con la intención de que los padres lo instalen en los ordenadores de sus hijos.
- En Windows y MacOS, Chrome desactiva las extensiones que no estén alojadas en el sitio web Chrome Web Store.

Por ejemplo, una extensión fue excluida de Chrome Web Store y desactivada permanentemente en más de 40.000 ordenadores.

- Google censuró la instalación del bloqueador de anuncios de Samsung en teléfonos Android, aduciendo que bloquear anuncios es una «interferencia» con los anunciantes (que vigilan al usuario mediante los anuncios).

El bloqueador de anuncios es software privativo, igual que el programa Google Play que Google usa para denegar el acceso para instalarlo. Usar un programa que no es libre le da a su dueño poder sobre usted, y Google ha ejercido ese poder.

La censura de Google, a diferencia de la de Apple, no es total. Android permite que el usuario instale aplicaciones de otras formas. Usted puede instalar los programas libres de f-droid.org.

DRM

Gestión digital de restricciones, o «DRM», se refiere a las funcionalidades diseñadas para restringir lo que los usuarios pueden hacer con los datos de sus ordenadores.

- Google ahora permite que las aplicaciones de Android detecten si un dispositivo ha sido *rooteado*, y en ese caso, rechazar la instalación. La aplicación Netflix utiliza esta posibilidad para imponer el DRM, rechazando su instalación en dispositivos Android *rooteados*.

Actualización: Google ha cambiado *intencionadamente* Android para que las aplicaciones puedan detectar dispositivos *rooteados* y no se ejecuten en ellos. La aplicación de Netflix es *malware* privativo, y no debe utilizarse. En cualquier caso, esto no implica que lo que ha hecho Google sea menos malo.

- Chrome aplica el DRM. Al igual que Chromium, mediante software que no es libre y que forma parte efectiva de la aplicación.

Más información.

- Android contiene servicios específicos para el funcionamiento del DRM.

Fallos de seguridad

Estos fallos no son, o no fueron, intencionados, así que, al contrario que en el resto de este artículo, no deben ser considerados *malware*. Se mencionan aquí para refutar la suposición de que ese prestigioso software privativo no presenta fallos graves.

- Muchas aplicaciones de Android pueden rastrear los movimientos del usuario incluso cuando este no les permite obtener datos de localización.

Al parecer se trata de un defecto no intencionado de Android, aprovechado intencionalmente por aplicaciones maliciosas.

- La NSA puede pinchar los *smartphones* para obtener datos, incluidos iPhone, Android y BlackBerry. Aunque en el artículo no se ofrece mucho detalle, parece que no se utiliza la conocida puerta trasera universal que tienen prácticamente todos los teléfonos móviles. Puede tratarse de la explotación de varios fallos. Hay muchos fallos en el software de la radio de los teléfonos.

Interferencias

En esta sección se ofrecen ejemplos de software de Google que importuna, molesta o causa problemas al usuario. Estas acciones son parecidas al sabotaje, pero la palabra «sabotaje» es demasiado fuerte para referirse a ellas.

- Google está modificando Chromium a fin de que las extensiones no puedan alterar o bloquear nada de lo que contenga la página. Cabe la posibilidad de que los usuarios reviertan este cambio en una bifurcación de Chromium, pero seguro que Chrome (que no es libre) mantendrá el mismo cambio, y ahí los usuarios no podrán hacer nada.

Sabotaje

Los perjuicios indicados en esta sección no son precisamente *malware*, ya que no implica que un programa se ejecute de forma que perjudique al usuario. Pero se parecen mucho al *malware*, al tratarse de acciones técnicas de Google que perjudican a usuarios de cierto software específico de Google.

- Revolv es un dispositivo que controlaba las operaciones de una «casa inteligente»: encender las luces, poner en funcionamiento los sensores de movimiento, regular la temperatura, etc. Su software privativo depende de un servidor remoto para llevar a cabo esas tareas. El 15 de mayo de 2016, Google/Alphabet lo dejó intencionadamente fuera de uso al cerrar el servidor.

Si fuera software libre, los usuarios tendrían la posibilidad de ponerlo de nuevo en funcionamiento, de manera diferente, y entonces tendrían una casa que respeta la libertad en lugar de una casa «inteligente». No permita que el software privativo controle sus dispositivos y los convierta en ladrillos de 300 dólares sin garantía. ¡Exija ordenadores autónomos que utilicen software libre!

- Durante mucho tiempo, Google ha dispuesto de una puerta trasera para desbloquear de forma remota los dispositivos Android, salvo que el disco estuviera encriptado, algo que es posible desde Android 5.0 Lollipop, pero que todavía no es una opción activada por defecto.

Vigilancia

- El «Asistente» de Google graba las conversaciones de los usuarios incluso cuando se supone que no está a la escucha. Así, cuando un subcontratista de Google divulgó un millar de grabaciones de voz confidenciales, a partir de ellas se pudo identificar fácilmente a los usuarios.

Puesto que el «Asistente» de Google utiliza software privativo, no hay modo de saber o controlar lo que graba o transmite.

En lugar de tratar de mejorar el control del uso de las grabaciones, lo que Google debe hacer es no grabar ni escuchar la voz de la gente. Solo debería captar las órdenes que el usuario quiere dar a algún servicio de Google.

- Google Chrome es un instrumento de vigilancia. Permite que miles de rastreadores invadan los ordenadores de los usuarios e informen de las páginas que visitan a empresas de publicidad y de datos, y en primer lugar a Google. Es más, si los usuarios tienen cuenta en Gmail, Chrome los conecta automáticamente a ella para mejorar la elaboración de su perfil. En Android, Chrome informa también a Google de su localización.

El mejor modo de evitar la vigilancia es cambiarse a IceCat, una versión modificada de Firefox con algunos cambios para proteger la privacidad de los usuarios.

- Google rastrea los movimientos de los teléfonos Android y de los iPhones que ejecutan aplicaciones de Google, y a veces guarda los datos durante años.

Un software privativo presente en el teléfono debe de ser el responsable de enviar los datos de localización a Google.

- Google invita a la gente a permitirle monitorear su uso del teléfono, y todo el uso que se hace de internet en sus hogares, a cambio de un extravagante pago de 20 dólares.

Esta no es una función maliciosa de un programa que tiene algún otro propósito; ese es el único propósito del software, y Google así lo dice. Pero Google lo dice de tal manera que induce a la mayoría de los usuarios a ignorar los detalles. Creemos que esto hace que podamos incluirlo aquí.

- En un teléfono Android se ha observado que rastreaba la localización incluso en modo avión. Mientras estaba en modo avión no enviaba los datos de localización. En lugar de eso, guardaba los datos y los enviaba después.
- Algunas aplicaciones de Google para Android registran la ubicación del usuario incluso cuando este ha desactivado la opción de «seguimiento de la ubicación».

Hay más formas de desactivar otros tipos de seguimiento de la ubicación, pero la mayoría de los usuarios acabarán confundidos por lo engañosos que resultan los menús de configuración.

- Android rastrea la ubicación para Google incluso cuando los «servicios de ubicación» están desactivados, e incluso cuando el teléfono no tiene tarjeta SIM.

- Los Chromebooks económicos para escuelas recopilan muchos más datos de los estudiantes que los necesarios, y los almacenan indefinidamente. Padres y estudiantes se quejan de la falta de transparencia por parte de los servicios educativos y las escuelas, de la dificultad de renunciar a esos servicios y de la falta de políticas de privacidad apropiadas, entre otras cosas.

Pero quejarse no es suficiente. Padres, estudiantes y profesorado han de darse cuenta de que el software que Google utiliza para espiar al alumnado no es libre, de modo que no pueden comprobar qué hace realmente. La única solución es persuadir al equipo directivo de la escuela de que utilice exclusivamente software libre tanto en las aulas como para sus tareas administrativas. Si la escuela se gestiona de forma independiente, los padres y el profesorado pueden exigir a sus representantes en el Consejo escolar que rechacen el presupuesto a menos que la escuela ponga en marcha la transición al software libre. Si la gestión es de ámbito nacional, tendrán que persuadir a los legisladores (p. ej., a través de organizaciones de software libre, partidos políticos, etc.) de que los centros educativos públicos migren al software libre.

- La nueva aplicación de mensajería por voz de Google registra todas las conversaciones.
- Google Play (un componente de Android) rastrea los movimientos del usuario sin su permiso..

Incluso aunque usted desactive Google Maps y el rastreo de la ubicación, debe desactivar el propio Google Play para detener completamente el seguimiento. Este es otro ejemplo de cómo el software privativo finge obedecer al usuario, cuando realmente lo que está haciendo es otra cosa. Esto es algo impensable con software libre.

- Google Chrome facilita que las extensiones fisgoneen la navegación del usuario, y muchas así lo hacen.
- Google Chrome incluye un módulo que activa el micrófono y transmite el audio a sus servidores.
- Los termómetros Nest envían multitud de datos sobre el usuario.
- Google Chrome espía el historial de navegación, las afiliaciones, y otro software instalado.
- Software espía en teléfonos Android (¿y en portátiles con Windows?): The Wall Street Journal (en un artículo al que solo se puede acceder previo pago) informa que el FBI puede activar de forma remota el GPS y el micrófono en teléfonos y con Android y portátiles (es de suponer que portátiles con Windows). Aquí hay más información.
- Algunos dispositivos Android contienen software espía. Algunos teléfonos Motorola, fabricados cuando la compañía pertenecía a Google, utilizan una versión modificada de Android que manda datos personales a Motorola.
- Un teléfono Motorola está permanentemente a la escucha de las señales de voz.
- De forma intencionada, Google Play envía a los desarrolladores de

aplicaciones los datos personales de los usuarios que instalan la aplicación.

Pedir simplemente el «consentimiento» de los usuarios no es suficiente para legitimar acciones como esta. Actualmente, la mayoría de los usuarios han dejado de leer los «Términos y Condiciones» que explican en detalle lo que están «consintiendo». Google debe identificar de forma clara y honesta la información que recopila sobre los usuarios, en lugar de ocultarla en un oscuro acuerdo de licencia de usuario.

En cualquier caso, para proteger realmente la privacidad de la gente, ¡lo primero que hay que hacer es evitar que Google y otras empresas obtengan esta información personal!

- Muchas páginas web informan a Google sobre sus visitantes mediante el servicio Google Analytics, que indica a Google la dirección IP y la página visitada.
- Google Chrome contiene un registrador de teclas que envía a Google, tecla por tecla, todas las URL escritas en el teclado.

Tiranos

Tiranos son sistemas que rechazan cualquier sistema operativo que no esté «autorizado» por el fabricante.

- Motorola, cuando pertenecía a Google, fabricó teléfonos Android que son tiranos (aunque alguien encontró la manera de quebrar la restricción). Afortunadamente, la mayoría de los dispositivos Android no son tiranos.

ARRIBA ▲

Copyright © 2017, 2018, 2019 Free Software Foundation, Inc.

Esta página está bajo licencia Creative Commons Reconocimiento 4.0 Internacional.

Traducción: Daniel Gutiérrez, 2019. Revisiones: Equipo de traductores al español de GNU.